Privacy Highlights from State of the Net

JANUARY 26, 2016

No blizzard could stop the 2016 State of the Net Conference, which convened on Monday in Washington to address a wide array of Internet policy questions. Despite a truncated schedule, several prominent data security and privacy issues were raised throughout the conference, including the future of US-EU Safe Harbor and how to secure consumer information while addressing the "going dark" debate around encryption policy.

Safe Harbor 2.0

With a looming deadline to establish a new Safe Harbor framework, everyone in the room had something to say about the future of transatlantic data transfers. FTC Commissioner Terrell McSweeny admitted that there were "a legitimate set of legal differences" standing in the way but remained optimistic that a deal could be struck. However, she conceded that the Snowden revelations and US surveillance policies remained unresolved questions with regards to the Safe Harbor.

Justin Antonipillai from the Department of Commerce explained that one of the key aims of the interagency group negotiating the new Safe Harbor is to educate the European Commission about "the limitations and safeguards our intelligence community, national security, and law enforcement elements operate under." Discussing the proposed Judicial Redress Act, Antonipillai stated that Commerce was committed to pursuing multiple privacy remedies for EU citizens.

Andrea Glorioso, counselor to the European Union Delegation, offered a "rebuttal" of sorts to Antonipillai. He noted that a revision to the Safe Harbor should be expected, as the framework was over 15 years old and no longer reflected existing data practices. Glorioso reaffirmed the importance of the Judicial Redress Act and cautioned that the Safe Harbor's reliance on FTC enforcement was also problematic, due to its status as an independent agency that cannot legally be bound to do anything under any Safe Harbor framework.

As for the man who instigated this debate, Max Schrems suggested European countries were just as culpable as the United States with respect to mass surveillance. He considered a challenge before the European Court of Justice against companies sharing data with *European* intelligence agencies and law enforcement in light of European surveillance efforts would make for "a very

interesting case." "I'd love to bring it," he said.

What's Next for Data Security

Last but not least, policymakers continued to debate the best approach to securing consumer data. Assistant Attorney General Leslie Caldwell stated that digital privacy and encryption were important tools but "not a cure-all—especially when it impedes our ability to protect ourselves and each other in the physical world." She continued to implore technology companies to work with the administration to ensure digital evidence is accessible to law enforcement.

However, FTC Commissioner McSweeny repeated her skepticism of mandatory backdoors. While she conceded that the debate has an important national security angle, she argued that weakening encryption would undermine everyone's digital security. She also suggested it could have serious consequences for consumer protection.

Finally, the Commissioner remains "deeply worried" about inadequate data security practices in general. Highlighting a recent article about an online search engine for vulnerable webcams, she strongly hinted that the FTC would be pursuing additional investigations and actions with respect to security efforts across the Internet of Things. She argued for more transparency into corporate security practices and encouraged efforts to help white hat security researchers evaluate everything from potential backdoors to the fairness of algorithms.